(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 283 630 A2

# (12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.02.2003 Bulletin 2003/07

(51) Int Cl.7: H04L 29/06, H04L 12/56

(21) Application number: 02017299.5

(22) Date of filing: 01.08.2002

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 07.08.2001 US 922642

(71) Applicant: ITT MANUFACTURING ENTERPRISES, INC.
Wilmington, Delaware 19801 (US)

(72) Inventors:
- Haight, Charles F.
Pine Brook, New Jersey 07058 (US)
- Bertrand, John
Upper Nyack, New York 10960 (US)

(74) Representative: Verscht, Thomas K.
Agnesstrasse 64
80797 München (DE)

## (54) Network routing using an untrusted router

(57) A trusted guard unit is used in a red/black secure environment to enable an untrusted router to be used to generate routing information for confidential data. The trusted guard generates a dummy message by substituting dummy data for confidential data in a message to be routed from a red environment to a black environment. The dummy message is sent to an untrusted router to generate routing information for use in routing the confidential data, but without the untrusted router receiving the confidential data. Another trusted guard receives from the router the dummy message with the routing information, and substitutes the confidential data for the dummy data in the dummy data message to generate a transmission frame to send to a destination node.

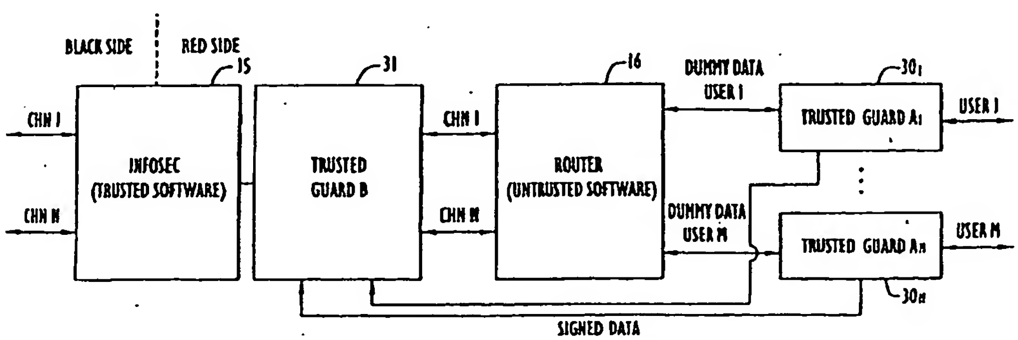



FIG. 6

EP 1 283 630 A2

Printed by Jouve, 75001 PARIS (FR)

## Description

### BACKGROUND OF THE INVENTION

#### Field of the Invention

[0001] The invention relates to network communications methods and systems. More particularly, it relates to routing data of multiple levels of security in a data communication network.

#### Description of the Related Art

[0002] Over the past several years the world has witnessed tremendous advances in commercial networking technologies. Many of the advances concern routing techniques and devices used in commercial networks, and networks of networks often referred to as the Internet. Typically, commercial routers are used in unsecured environments, at least from a data perspective. That is, commercial routers have been developed for commercial use without regard to supporting information classified according to multiple levels of security. Although commercial routing devices typically undergo many reliability and quality tests, they are not designed, nor are they tested, with the goal of handling multiple levels of security classification.

[0003] In contrast to commercial environments, networking devices for use in military applications are often required to support multiple levels of security classification. Multilevel security (MLS), according to the *National Information Systems Security (INFOSEC) Glossary*, NSTISSI No. 4009, January 1999 (Rev. 1), is a concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. Multilevel security and MLS, as used here, encompass simultaneous access by users with different levels of access authority that is not necessarily limited to a national security clearance level.

[0004] Information classified according to a government or military organization's security classification is referred to here as classified information. Information used in a commercial environment and to which access is to be limited is referred to as proprietary information. More generally, confidential information refers to information to which access is to be limited and encompasses both classified and proprietary information.

[0005] In an MLS environment, it is important to use a trusted computing system, which refers to the totality of protection mechanisms within a computer system, including hardware, firmware, and software, that is, the combination responsible for enforcing an organization's security policy. In many trusted computing systems that process sensitive or classified information, especially national security information, information systems' security methods and devices are used to protect the information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. Such information systems often employ red/black concepts and techniques. "Red/black" refers to separation of electrical and electronic circuits, components, equipment, and systems that handle national security information (red) in electrical form from those that handle non-national security information (black) in the same form, as described in the *National INFOSEC Glossary*. Devices and software components that operate in a red environment for processing classified data undergo extensive testing to ensure the integrity of the classified data passing through those components. Such testing can be very lengthy and very expensive.

[0006] Unfortunately, because of the extensive design and testing to ensure the integrity of red data, many military computing systems have not been able to take full advantage of the tremendous advances in routing technology taking place in the commercial networking world. Accordingly, there is a need to use commercial networking equipment, particularly network routers, in computing environments that must support MLS systems, yet without requiring the extensive testing to certify that equipment to process red data. Hence, there is a need to employ untrusted commercial network routers in computing systems that handle multilevel security data.

[0007] A Joint Tactical Radio System (JTRS) software radio is an example of equipment that must operate in a MLS environment. A software radio is a radio that uses computer software to perform a variety of functions in the process of converting voice or data information to and from a radio frequency (RF) signal. The architecture of the JTRS software radio is designed, as shown in Fig. 1, in a modular manner in order to use commercial-off-the-shelf (COTS) components and thereby leverage COTS development and reduce the overall development costs of the JTRS software radio. The architecture depicted in Fig. 1 is a conceptual diagram illustrating major functional units, and does not necessarily illustrate physical relationships.

[0008] The software radio notional architecture shown in Fig. 1 includes a red critical system interconnect (CSI) 1 and a black CSI 2. The red CSI couples functional entity interfaces (FEI), such as a user interface 3 or a network interface 4, to various red FEI units. Those units can include a human-computer interface (HCI) 5, a red system control unit 6, an internetworking unit 7 and an information security (INFOSEC) unit 8. The red CSI allows various types of red FEI units to be used on the red side of the radio. For example, the internetworking unit 7, the red system control unit 6 and the HCI 5 can all reside on a single processor board 9, such as a Pentium class microprocessor circuit board that connects to the red CSI.

[0009] The INFOSEC unit 8 connects to the black CSI on the black side of the software radio, and to the red CSI on the red side of the radio, and forms a boundary between the red and black environments. Connected to the black CSI are an antenna I/O interface unit 10 for sending and receiving RF signals, RF units 11, modems 12, and various other black side processes 13. Also, a user interface 14 can be connected to the black CSI as shown in Fig. 1. The black CSI allows various types of COTS functional entity interface units to be used in the software radio, such as various types of commercial modems, for example.

[0010] The internetworking unit 7 includes a router for routing messages, received from the user interfaces on the red side of the radio or received over the air after black side INFOSEC processing, to destinations on either the red or black sides of the radio. For destinations on the black side of the radio, the router must send the messages through the INFOSEC 8.

[0011] A multiple-input, multiple-output information system capable for use in the JTRS software radio is shown in Fig. 2 in which the INFOSEC unit 15 forms a boundary between red and black environments. On the black side of the system the INFOSEC interfaces with input/output channels 1 through N. Similarly, on the red side of the system the INFOSEC interfaces with corresponding input/output channels 1 through N that connect to a router 16. The router 16 is coupled to a plurality of users, here, user 1 through user M. In such an environment the data streams may be at different security/. compartment levels if it is a government information system, or the data steams may belong to different communities of interest if in a commercial environment.

[0012] The router 16 receives data, either from a user or from one of the channels, and routes it to the appropriate destination. For example, user 1 may send a message addressed to a destination reached using channel N. The router 16, using routing tables and routing algorithm software, receives the message from user 1 and based on the address determines a route over which to send the message. This entails attaching routing information to the message and outputting the message over the channel the router determines services the chosen route. The router 16, through the use of its routing tables and algorithms, determines that the message is to be output on channel N, for example. Accordingly, the router outputs the message on channel N with the added routing information attached to the message. Similarly, when the router receives a message on one of the N channels, it examines the routing information in the received message, determines the user or channel to which to send the message, and outputs the message to that user or channel. Because the router 16 receives data streams that may be at different security/compartment levels (government system) or may belong to different communities of interest (commercial system), the router in Fig. 2 must be tested to ensure it can be trusted with those data streams.

[0013] It is highly desirable to use standard commercial software for the router because of the rapid technological advances and routing evolution occurring in the commercial sector. However, commercial routing software does not undergo the rigorous and extensive testing required to certify it as trusted and therefore a commercial router has no level of trust. Yet, there is a strongly felt need to develop an approach that uses commercial routing techniques and software in an MLS environment and guarantees that data from one security level will not get released to users or networks at a different level without following the safeguards specified by the information system's security policy.

## SUMMARY OF THE INVENTION

[0014] Therefore, in light of the above, and for other reasons that will become apparent when the invention is fully described, an object of the invention is to use a router that has not been certified to process data of multiple security levels, to provide routing information for a message containing confidential data.

[0015] A further object of the invention is to use routing information from an untrusted router to route confidential data without sending that data to the router.

[0016] Yet another object of the invention is to generate a transmission frame by combining routing information from a dummy message sent to a router, with confidential information to be transported using the transmission frame.

[0017] A still further object of the invention is to obtain routing information from a router that is not certified to handle information of multiple levels of security without sending confidential information to the router.

[0018] The aforesaid objects are achieved individually and in combination, and it is not intended that the invention be construed as requiring two or more of the objects to be combined unless expressly required by the claims attached hereto.

[0019] A method in accordance with the invention routes a data message containing confidential information, by substituting dummy information for the confidential information in the message. The message is sent with the dummy information to a router for adding routing information to the message, and the confidential information is elsewhere substituted for the dummy information in the message containing the routing information.

[0020] A trusted guard apparatus, according to the invention, sends a data message to a router, in which the data message has information classified at a first security level. The apparatus includes a source authentication unit configured to receive the data message containing the information classified at the first security level, and to add to the data message source information concerning the source of the data message. The apparatus also includes a data integrity unit coupled to the source authentication unit and configured to transform the information classified at the first security level to in-

clude information for determining the integrity of the information classified at the first security level. It also includes a data substitution unit coupled to the source authentication unit and configured to generate a dummy data message by substituting dummy data for the information classified at the first security level, and outputting the dummy data message to the router.

[0021] A transmission frame for delivering confidential data to a destination node, according to the invention, includes a dummy data field containing dummy data, classified at a first security level, substituted for confidential data classified at a second security level different from the first security level. The transmission frame also includes a message header field containing information identifying the destination node, and a routing field containing routing information for use in routing the transmission frame to the destination node.

[0022] The above and still further objects, features and advantages of the invention will become apparent upon consideration of the following descriptions and descriptive figures of specific embodiments thereof. While these descriptions go into specific details of the invention, it should be understood that variations may and do exist and would be apparent to those skilled in the art based on the descriptions herein.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0023]

Fig. 1 is a block diagram illustrating an architecture of a software radio.

Fig. 2 is a block diagram of a portion of a computing system, such as the software radio of Fig. 1, using a router and an INFOSEC.

Fig. 3 is a block diagram of a computing system using an untrusted router in combination with an INFOSEC and a trusted guard unit.

Fig. 4 is a diagram showing a detailed view of a trusted guard unit A.

Fig. 5 is a flowchart illustrating a process of routing data according to the invention.

Fig. 6 is a block diagram of a computing system using an untrusted router, a trusted guard unit and showing data flows according to certain aspects of the invention.

Fig. 7 is a detailed view of a trusted guard with a dummy message generator.

Fig. 8 is a detailed view of a trusted guard unit that combines routing information from an untrusted router with signed data from another trusted guard unit.

Figs. 9A-D are diagrams of data packets at various stages of a routing process according to aspects of the invention.

Fig. 10A-G are diagrams illustrating various data flows in a software radio.

## DETAILED DESCRIPTION

[0024] Preferred embodiments according to the present invention are described below with reference to the above drawings, in which like reference numerals designate like components.

[0025] When dealing with data processed by untrusted software between a source and a destination, it is necessary to prove at the destination point that the source information is accurate (source authentication) and that the data has not been modified (data integrity). If source authentication and data integrity are provided at the source and destination by trusted software and/ or hardware entities, referred to here as trusted guards, then the untrusted router cannot interfere undetected with that information that is sent from the source to the destination and the trusted entities can enforce the computing system's security policy.

[0026] Fig. 3 is a block diagram showing a trusted guard A 17 coupled with users 1 through M and coupled to ports 1 through M of the router 16. Another trusted guard B 18 is coupled to channels 1 through N of the router 16 and to the INFOSEC 15. Trusted guard B can be included as part of the INFOSEC 15.

[0027] A block diagram of trusted guard A is shown in Fig. 4. The trusted guard of Fig. 4 includes a labeling unit 19, a secure hashing algorithm (SHA) unit 20, a digital signature (DSS) unit 21 and a signature application unit 22. To provide source authentication the trusted guard's labeling unit 19 receives user data and source information and uses that information to attach a label to the data at its source. The label can include information about the source, such as, for example, a channel number, a security level, a packet number, the length of the packet and/or a time-of-day label. Further, if assurance requirements so dictate, the trusted guard can add other information to the data such as a packet number, a time stamp or a unique identifier such as an identifier cryptographically generated by a trusted guard. The trusted guards are initialized by the INFOSEC, preferably at the time of powering on the trusted guards. For example, the INFOSEC can initialize the trusted guards to operate at a specific security level depending on the guard's certification. The information provided by the labeling unit can be set at initialization. The SHA unit 20 can be used to reduce the amount of data by applying a hash algorithm to the labeled data and thereby reduce the computational complexity of the digital signature evaluation. Hashing can be used to reduce the complexity of using digital signatures, although it need not be used to practice the invention. The trusted guard can use well-known techniques to provide data integrity when sending data between trusted guards, such as by applying a digital signature to the labeled data. For example, a digital signature can be a number computed from the data being signed. An example of a digital signature is a check-sum computed from the data and label. Generally, however, a cryptographic procedure is

used instead of a checksum, to ensure that a signature cannot be modified. An example of such a cryptographic procedure that can be used to ensure the integrity of the data is the AFIPS-specified Digital Signature (DSS) which is based on Public Key Encryption. The DSS unit 21 shown in Fig. 4 determines and outputs such a digital signature for the labeled data. The signature application unit 22 applies the signature to the labeled data received from the labeling unit 19, and outputs the labeled data with the signature as signed data. The trusted guard B 18, connected to the INFOSEC as shown in Fig. 3, receives the signed and labeled data from the router 16, authenticates it and verifies its integrity by using the signature and label in the data.

[0028] The trusted guard system shown in Fig. 3 would suffice for routing messages to their destinations and ensuring that the security of the data is not compromised, if the untrusted router 16 were not allowed to generate data. If that were the case, and the router not allowed to generate data, the router would not be able to masquerade as a data source since the router could not generate signed data, as the source and destination are trusted and are the only ones that have the keys required by the DSS unit. However, the router 16 must be allowed to generate data, such as routing tables, and transmit them to other routers. Accordingly, the approach of labeling, hashing and signing data is insufficient to ensure that the router 16 cannot, through malicious or faulty software, hold on to data and then transmit that data as part of its own data transmissions, since that might cause data at a higher classification level to be released to users who are not authorized to see that data.

[0029] The invention allows a router with untrusted software to be used in an MLS environment, yet ensures that the router does not release data from one security level to users or networks at a different level. This involves diverting data around the router that has the untrusted software, while using the router to supply routing information. An overall general process for using an untrusted router in an MLS environment is illustrated in Fig. 5. The process begins by trusted guard A receiving a message routed from a data source (23). The data in the message, which might be confidential and classified with a security level higher than a security level at which the router is certified, is removed and replaced with dummy data, such as a predetermined pattern of characters that is non-confidential (24). Alternatively, a pseudo random pattern can be cryptographically generated by the sending guard and validated by the receiving guard. The message with the dummy data (i.e., a dummy data message) is sent to the router 16, and the data removed from the message is directed around the untrusted router 16 and sent to trusted guard B to eventually match it with the dummy message once the router 16 determines the routing information (25). The router 16 receives the dummy message, determines a route for it to travel to reach its intended destination, and appends to the dummy message routing information specifying such a route (26). The router sends the dummy message with the routing information to trusted guard B where the data is diverted (27). Trusted guard B then replaces the dummy data in the message to which the routing information is appended with the data from the data source (28). Trusted guard B then sends the reconstructed message according to the routing information supplied by the router (29). In this manner, a router 16 with untrusted software is used to supply routing information without the untrusted router receiving data from the data source.

[0030] The operation of the untrusted router system of Fig. 3 is modified to perform a data diversion technique, as illustrated in Fig. 6. In the system shown in Fig. 6 a trusted guard A 30, coupled to users 1 through M and to the router, receives a message with data for delivery to a destination specified by an address in a header of the message. A detailed view of trusted guard A 19 is shown in Fig. 7. In addition to the trusted guard shown in Fig. 4, trusted guard A 30 also includes a dummy message generator 32. Trusted guard A 30, as described above, labels and applies a signature to the data. Alternatively, the trusted guard A compresses the labeled data using a hash algorithm or another data compression technique. Trusted guard A 30 sends the signed data (i.e., data + label + signature) over a trusted path that does not include the router, to a trusted guard B 31 that is coupled to the router 16 and INFOSEC 15. The dummy generator 32 receives the message supplied to trusted guard 30 from the user and replaces the data in the message with non-confidential dummy data that is classified at a security level the same as or lower than the security level of the router, and retains any headers in the message. An example of such non-confidential data is a predetermined pattern of characters or a pseudo random pattern that is cryptographically generated. Alternatively, the dummy message generator 32 can receive the message at any point in the trusted guard, so long as the message's header remains intact. Trusted guard A 30 then outputs the dummy message having the headers and non-confidential dummy data, to the router 16.

[0031] The router 16 receives the dummy message and based on the headers in the message determines a route for delivering the message to the intended destination. The router 16 then applies to the dummy message routing information specifying the determined route. For example, the router can apply the routing information by appending it to the dummy message. The router 16 then outputs the dummy message with the routing information to trusted guard B 31.

[0032] Trusted guard B 31 is shown in detail in Fig. 8 and includes a dummy message receiving unit 33, a signed data receiving unit 34, a message reconstruction unit 35, and an output unit 36. Signed data receiving unit 34 receives the signed data sent from the trusted guard A 30 and sends it to the message reconstruction unit 35

which holds it until the dummy message receiving unit 33 receives the corresponding dummy message from the router 16. The message reconstruction unit 35 then receives the signed data, matches headers, and replaces the dummy data with the signed data to form a reconstructed message. The reconstructed message includes the routing information, any original message headers and the signed data. The output unit 36 then outputs the reconstructed message to the INFOSEC 15, which performs conventional red/black isolation functions, and forwards the message to the intended destination along a path specified by the routing information.

[0033] Since the source and destination are trusted and are the only ones that have the keys required by the digital signature algorithms, the destination upon receiving the message uses its keys to unhash and authenticate the message. In this manner the message is routed and verified at the destination.

[0034] Trusted guard A can include the same structure and perform the same functions as trusted guard B, shown in Fig. 8, where trusted guard A also receives data from another trusted guard. Likewise, trusted guard B can include the same structure and perform the same functions as trusted guard A, shown in Fig. 7, where trusted guard B also sends data to another trusted guard.

[0035] Figs. 9A-9D show examples of messages sent from the source through the trusted guard A and the untrusted router to the INFOSEC. A user, for example user 1 shown in Fig. 6, sends a message shown in Fig. 9A that contains data 38 that could be confidential and classified at a security level higher than a level at which the router is certified. The message in Fig. 9A also includes standard headers (HDR) 37 attached to the confidential data according to the networking protocols in use. Trusted guard 30, upon receiving the confidential data substitutes dummy data 39 for the confidential data and sends a dummy message, shown in Fig. 9B, to the router 16. The router 16, upon receiving the dummy message adds a routing header 40 to the dummy data 39 and header 37. The routing header 40 includes routing information for routing the message to the destination. The router 16 sends the dummy data message with the routing header, shown in Fig. 9C, to trusted guard B 31 by way of the appropriate channel according to the determined route.

[0036] Trusted guard A 30 sends the confidential data 38 that has been separated from the original message to trusted guard B 31. As discussed above, trusted guard A 30 can apply a hashing function to the confidential data, and can also apply a digital signature to the data. Trusted guard A 30 sends the signed confidential data to trusted guard B 31 by way of a trusted path separate from the router.

[0037] Trusted guard B 31 matches the signed data with the dummy message received from the router that contains the routing header 40. Trusted guard B 31 substitutes the signed confidential data 38 received from the trusted guard A 30 for the dummy data 39 contained in the message received from the router16. Thus, trusted guard B 31 forms the message, or transmission frame, shown in Fig. 9D that includes the routing header 40 that contains the routing information for delivering the message to the intended destination, the original headers 37 and the confidential data 38. Trusted guard B 31 then sends the message shown in Fig. 9D to the INFOSEC for transmission to the destination along the determined route. The process described above also operates in the reverse direction. When information arrives from channels 1 through N it is provided to one of the users 1 through M. In that case, trusted guards A and B operate with their roles reversed.

[0038] The trusted guards described above can be used in a variety of data flow scenarios for delivering data both to the red side and the black side of INFOSEC 15. Various such data flows are shown in Figs. 10A through 10G, in which the data flows represented by a solid line designate messages that contain data from a source, such as red data from a user. The dashed lines depict data flow of messages containing dummy data.

[0039] The data flow shown in Fig. 10A depicts a message originating from the red side of the INFOSEC and flowing to a destination on the black side. Here, a user A sends a message containing red data through the user A's I/O device 3A to a trusted guard 30A and over the red bus 1 to trusted guard 31 to INFOSEC 15 for delivery to a destination over black bus 2. In the manner described above, trusted guard 30A substitutes dummy data for the red data in the message to create a dummy message. Trusted guard 30A sends the dummy message to untrusted router 16 which adds routing information to the dummy message, as depicted by the dashed line. The router 16 sends the dummy message with the routing information to trusted guard 31. Meanwhile, trusted guard 30A sends the message data to the trusted guard 31 across red bus 1, as depicted by the solid line. Trusted guard 31 then reconstructs the message by combining the routing information in the dummy message with the red data received from trusted guard 30A. Trusted guard 31 then sends the reconstructed message to the INFOSEC for delivery to a transmitter on the black bus 2.

[0040] Data flowing in the reverse direction is shown in Fig. 10B. Here, a message sent from a source outside the local red environment shown in Fig. 10B is received by INFOSEC 15 from black bus 2. In the case of the JTRS software radio the message, likely in the form of a data packet, is received by the radio's antenna and demodulated on the black side of the INFOSEC 15. The demodulator forwards the message to the INFOSEC 15 over the black bus 2 and the INFOSEC 15 passes the received message to trusted guard 31. The trusted guard 31 generates a dummy message with the header information from the received message and dummy data substituted for the data in the message, and forwards the dummy message to untrusted router 16, as depicted

by the dashed line. The INFOSEC 15 decrypts the message's data and passes the decrypted data to trusted guard 31. The router 16 returns the I/O address for the destination to the trusted guard 31. In the example shown in Fig. 10B the router returns the I/O address for user A's I/O device 3A. The trusted guard 31 then verifies the messages destination, and assembles the decrypted data with the header information returned from the router. Before sending the decrypted data to the destination I/O device indicated by the header information returned from the router, the trusted guard 31 verifies that the indicated destination is authorized to receive information at the security level of the decrypted data. Once verified the trusted guard 31 hashes and signs the message and sends the assembled message with the decrypted data to the destination I/O device via the red bus 1, here, user A's I/O device 3A, as depicted by the solid line.

[0041] Alternatively, the data flow shown in Fig. 10B can be achieved by router 16 forwarding the dummy message to the trusted guard servicing the destination I/O device as shown in Fig. 10C. Here, trusted guard 31 places the data from the received message on the red bus 1 with some type of identifier, such as, for example, a packet number, date/time stamp, etc. The dummy message generated by trusted guard 31 would have the same identifier (e.g., packet number, date/time stamp, etc.). All trusted guards on red bus 1 would see the data placed on the red bus, but only the guard(s) to which the dummy message is sent will take the data off the red bus and supply it to the respective user I/O device. The trusted guard(s) that receive the dummy message can detect the corresponding data on the red bus by matching the identifiers (e.g., packet number, date/time stamp, etc.) In the example shown in Fig. 10C, user A's I/O device 3A receives the dummy message thus indicating that it is to receive the data placed on the bus. Trusted guard 30A then matches identifying information from the dummy message with the data on the red bus, and if there is a match it takes the data off the red bus, authenticates it and supplies the data to user A's I/O device 3A. The other trusted guards ignore the data on the red bus because they did not receive the dummy message from the router 16. The other trusted guards also ignore the data, if the data is labeled, because the attached label does not indicate that the data is destined for them.

[0042] Fig. 10D depicts a data flow for the case in which a message is routed only within the red environment of the communication system. In Fig. 10D user A sends a message, via user A's I/O device 3A, to user B. Trusted guard 30A receives the message from user A's I/O device 3A and substitutes dummy data for the red data in the message. The dummy message is sent to untrusted router 16 for application of routing information to the message, as depicted by the dashed line. Trusted guard 30A sends the message's red data to the INFOSEC 15 by way of trusted guard 31. The router 16 adds routing information to the dummy message and then sends it to the trusted guard that services INFOSEC 15, i.e., trusted guard 31. If the message's destination is local, that is, within the red environment shown in Fig. 10D, and the encryption requirements are the same for both users (e.g., not requiring radio transmission), then the message need not be sent to INFOSEC 15 for encryption/decryption services. Accordingly, trusted guard 31 reconstructs the message by assembling the red data with the header information received from the untrusted router 16 that contains the routing information. Trusted guard 31 forwards the reconstructed message data and header to the destination user I/O device indicated in the routing information, as depicted by the solid line. In the example shown in Fig. 10D the message is destined for user B, and accordingly, the reconstructed message is forwarded to user B's I/O device 3B via trusted guard 30B. Before allowing the message data to be released to user B's I/O device, the trusted guard 30B verifies that the data in the message is at the proper classification level for the destination indicated by the routing information.

[0043] Alternatively, in situations where security access controls do not require the function of INFOSEC 15, the message can be routed without sending the data to either the router 16 or the INFOSEC 15. In that case, depicted in Fig. 10E, when sending a message between users in the same red environment the untrusted router 16 upon receiving the dummy message and determining the appropriate routing information can notify the destination trusted guard, in this example, trusted guard 30B, that the message is intended for user B. The router 16 can notify the destination trusted guard by sending it the dummy data message, as shown by the dashed line in Fig. 10E, with the routing information included in that message. This notification can occur by the router 16 routing the dummy data message to the destination. When the source trusted guard, in this example, trusted guard 30A, substitutes dummy data for the message data, it can place the message data on the red bus 1 for all trusted guards to see, as shown by the solid line. As described above, trusted guard 30A can add identifying information to both the dummy data message and the message data to facilitate later matching. Only the trusted guard receiving the dummy data message from the router, here trusted guard 30B, will then identify the data on the red bus 1 as matching the dummy data message and take the message data off of red bus 1. The destination trusted guard can verify and authenticate the data, and allow the message data to be passed to user B only if user B is authorized to access the message data.

[0044] Another data flow example is shown in Fig. 10F. In this example the data path is the same as shown in Fig. 10D except the encryption/decryption requirements are different. That is, here, user A sends a message intended for user B, however the message must be encrypted due to channel setup requirements designated at instantiation. Here, trusted guard 30A separates the message data from the message's header in-

formation and uses that header information to generate a dummy message containing dummy data. The dummy message, with the message's header information, is sent to untrusted router 16 to add routing information, as shown by the dashed line. The message data is supplied to INFOSEC 15 via trusted guard 31, as shown by the solid line. The untrusted router, upon determining the appropriate route, provides the routing information to trusted guard 31, preferably in the form of routing information added to the header of the dummy message. The untrusted router 16 then sends the dummy message to trusted guard 31, as depicted by the dashed line. In this example the message must be encrypted or decrypted since the user's encryption/decryption requirements are different. INFOSEC 15 performs the appropriate encryption/decryption on the message data according to the channel setup requirements for users A and B, and supplies the appropriately encrypted or decrypted message data to trusted guard 31. Trusted guard 31 then adds the routing information supplied by untrusted router 16 to the message data that is to be delivered to user B, thereby reconstructing the message. The trusted guard 31 sends the reconstructed message to user B according to the routing information, as depicted by the solid line. Trusted guard 30B receives the reconstructed message and verifies and authenticates the message before supplying it to user B's I/O device 3B.

[0045] Alternatively, the data flow depicted in Fig. 10F can be accomplished in other ways. For example, as shown in Fig. 10G, trusted guard 30A can send the message data to the INFOSEC 15, as depicted by the solid line, for encryption/decryption. The INFOSEC 15, after encrypting/decrypting the message data, can place that data on red bus 1 via trusted guard 31. The router 16 can notify the destination trusted guard of the message, such as by sending the dummy message to the destination trusted guard, in this example, trusted guard 30B, as depicted by the dashed line. The destination trusted guard, here, trusted guard 30B, upon receiving the dummy message matches identifying information in the dummy message with identifying information in the data on the red bus. If they match trusted guard B takes the encrypted/decrypted data off of red bus 1. Trusted guard 30B then verifies and authenticates the message data and supplies it to user B's I/O device if it's security level is adequate for the security classification of the message data.

[0046] It will be understood that the functions of the trusted guards, and the units within the trusted guards such as the units shown in Figs. 7 and 8, can be performed using computer programs controlling computer hardware and firmware. It will also be understood that such computer programs can be recorded on computer-readable media, such as magnetic and optical disks, and can be transmitted in a computer-readable signal.

[0047] Having described preferred embodiments of network routing using an untrusted router, it is believed that other modifications, variations and changes will be suggested to those skilled in the art in view of the teachings set forth herein. It is therefore to be understood that all such variations, modifications and changes are believed to fall within the scope of the present invention as defined by the appended claims. Although specific terms are employed herein, they are used in their ordinary and accustomed manner only, unless expressly defined differently herein, and not for purposes of limitation.

**Claims**

1. A method of generating a transmission frame for routing a first message, the first message having a header and first data, the method comprising:

    generating a second message by substituting second data for the first data in the first message;
    adding routing information to the second message; and
    generating the transmission frame by substituting the first data for the second data in the second information message after the routing information is added to the second information message.

2. The method of item 1, wherein the header in the first message identifies a destination for the first message.

3. The method of item 1 or 2, further comprising sending the transmission frame to the destination according to said routing information.

4. The method of any of items 1 to 3, wherein the first data is classified at a first security level and the second data is classified at a second security level different from the first security level.

5. The method of item 4, wherein the first security level is a security level designated for information to which access is restricted and the second security level is a security level designated for information to which access is not restricted.

6. The method of any of items 1 to 5, wherein the second data is a predetermined pattern of characters.

7. A method of routing a data message containing confidential information, the method comprising:

    substituting dummy information for the confidential information in the message;
    sending the message with the dummy information to a router for adding routing information to

the message; and
outputting the confidential information for substitution with the dummy information after the routing information is added to the message.

8. The method of item 7, further comprising sending the message with the confidential information substituted for the dummy information to a destination node indicated by the routing information.

9. A computer program product directly loadable into the internal memory of a (digital) computer, the computer program product for controlling a computerized device to route a data message containing confidential information when said computer program product is run on a computer, the computer program product comprising:

program code for substituting dummy information for the confidential information in the message;
program code for sending the message with the dummy information to a router for adding routing information to the message; and
program code for outputting the confidential information for substitution with the dummy information after the routing information is added to the message.

10. The computer program product of item 9, further comprising program code for sending the message with the confidential information substituted for the dummy information to a destination node indicated by the routing information.

11. A trusted guard apparatus for sending a data message to a router, the data message having information classified at a first security level, the apparatus comprising:

a source authentication unit configured to receive the data message containing the information classified at the first security level, and to add to the data message source information concerning the source of the data message;
a data integrity unit coupled to the source authentication unit and configured to transform the information classified at the first security level to include information for determining the integrity of the information classified at the first security level; and
a data substitution unit coupled to the source authentication unit and configured to generate a dummy data message by substituting dummy data for the information classified at the first security level, and outputting the dummy data message to the router.

12. The trusted guard apparatus of item 11, wherein information classified at the first security level is confidential information and the dummy data is non-confidential information.

13. The trusted guard apparatus of item 11 or 12, wherein the data integrity unit transforms the information classified at the first security level by applying a digital signature to said information.

14. The trusted guard apparatus of any of items 11 to 13, wherein the information concerning the source of the data message added by the source authentication unit is a label identifying the source of the data message.

15. The trusted guard apparatus of any of items 11 to 14, further comprising a compression unit coupled to the source authentication unit and configured to compress the information classified at the first security level.

16. The trusted guard apparatus of item 15, wherein the compression unit is configured to compress the labeled data by applying a secure hashing algorithm to the information classified at the first security level.

17. A trusted guard apparatus for sending a data message to a router, the data message having information classified at a first security level, the apparatus comprising:

a source authentication unit configured to receive the data message containing the information classified at the first security level, and to add to the data message source information concerning the source of the data message;
a data integrity unit coupled to the source authentication unit and configured to transform the information classified at the first security level to include information for determining the integrity of the information classified at the first security level; and
means for generating a dummy data message by substituting dummy data for the information classified at the first security level, and outputting the dummy data message to the router.

18. The trusted guard apparatus of item 17, wherein information classified at the first security level is confidential information and the dummy data is non-confidential information.

19. The trusted guard apparatus of item 17 or 18, wherein the data integrity unit transforms the information classified at the first security level by applying a digital signature to said information.

20. The trusted guard apparatus of any of items 17 to 19, wherein the information concerning the source of the data message added by the source authentication unit is a label identifying the source of the data message.

21. The trusted guard apparatus any of items 17 to 20, further comprising a compression unit coupled to the source authentication unit and configured to compress the information classified at the first security level.

22. The trusted guard apparatus of item 21, wherein the compression unit is configured to compress the labeled data by applying a secure hashing algorithm to the information classified at the first security level.

23. A transmission frame for delivering confidential data to a destination node, comprising:

   a dummy data field containing dummy data classified at a first security level, substituted for confidential data classified at a second security level different from the first security level;
   a message header field containing information identifying the destination node;
   a routing field containing routing information for use in routing the transmission frame to the destination node.

24. The transmission frame of item 23, wherein access to data classified at the first security level is restricted, and access to data classified at the second security level is unrestricted.

25. A method of generating a transmission frame for routing a message containing confidential data to a destination node, the method comprising:

   receiving a dummy data message containing routing information specifying a route to the destination node, and dummy data substituted for the confidential data;
   receiving the confidential data separately from the dummy data message; and
   substituting the confidential data for the dummy data in the dummy data message thereby generating the transmission frame.

26. The method of item 25, wherein the confidential data is classified at a security level at which access is restricted, and the dummy data is classified at a security level at which access is not restricted.

27. A trusted guard apparatus for routing a data message to a destination node, the data message including confidential information, the apparatus comprising:

   a dummy message receiving unit coupled to a router and configured to receive from the router a dummy message containing dummy data and routing information for routing the dummy data message to a destination node;
   a confidential data receiving unit coupled to a trusted guard unit and configured to receive from the trusted guard unit the confidential data to be routed to the destination node; and
   a message reconstruction unit connected to the dummy data message and confidential data receiving units, wherein in response to receiving the dummy data message and the confidential data the message reconstruction unit generates an output message containing the routing information and the confidential data.

28. The trusted guard apparatus of item 27, further comprising an output unit configured to send the output message to the destination node based on the routing information.

29. A trusted guard apparatus for routing a data message to a destination node, the data message including confidential information, the apparatus comprising:

   means for receiving from a router a dummy message containing dummy data and routing information for routing the dummy data message to a destination node;
   means for receiving from the trusted guard unit the confidential data to be routed to the destination node; and
   means for substituting confidential data for the dummy data in the dummy data message thereby generating an output message containing the routing information, the confidential data.

30. The trusted guard apparatus of item 29, further comprising means for sending the output message to the destination node based on the routing information.

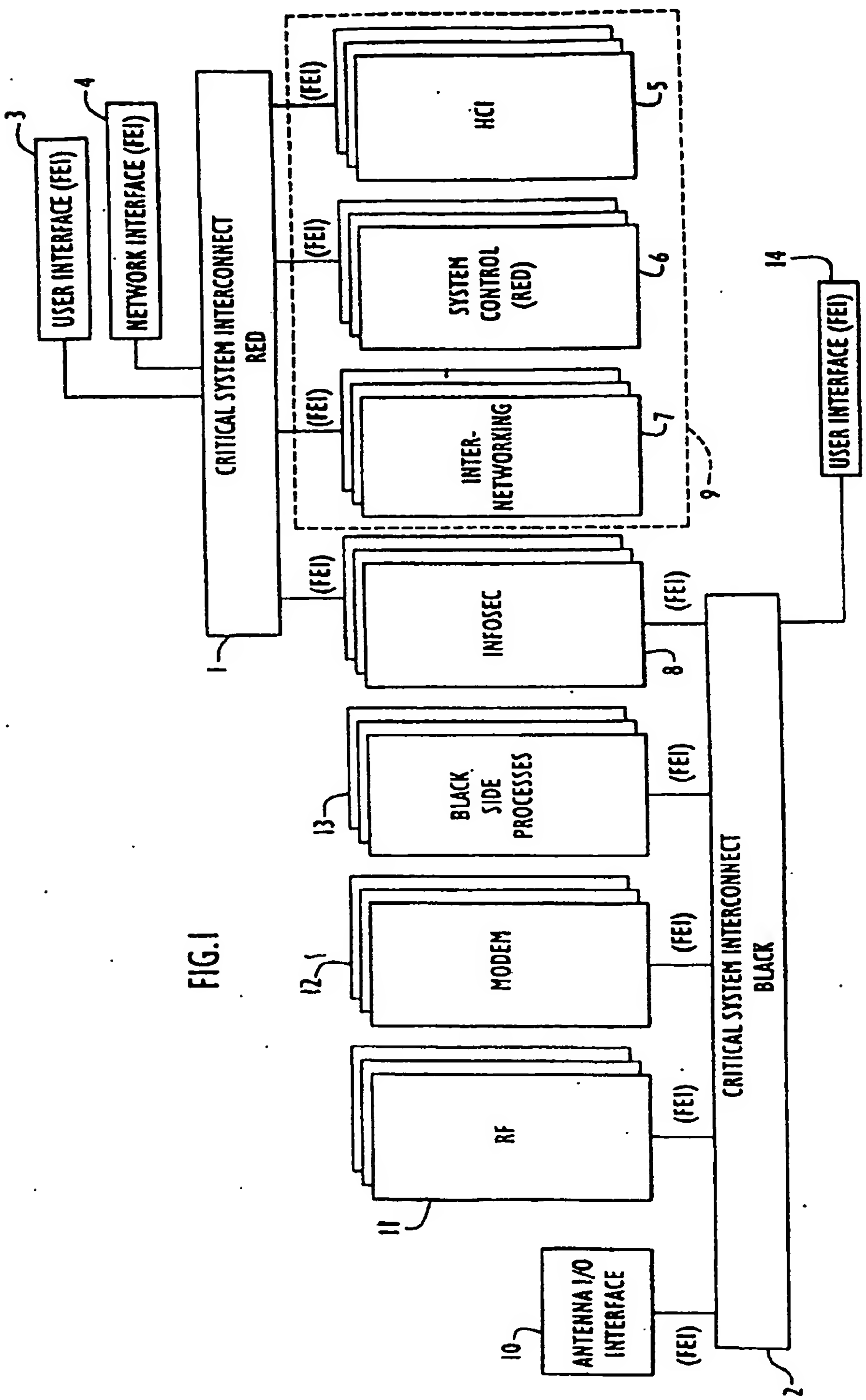

USER INTERFACE (FEI)
NETWORK INTERFACE (FEI)
CRITICAL SYSTEM INTERCONNECT RED
(FEI)
HCI
SYSTEM CONTROL (RED)
INTER-NETWORKING
INFOSEC
BLACK SIDE PROCESSES
MODEM
RF
ANTENNA I/O INTERFACE
CRITICAL SYSTEM INTERCONNECT BLACK
USER INTERFACE (FEI)
1
2
3
4
5
6
7
8
9
10
11
12
13
14

FIG.1

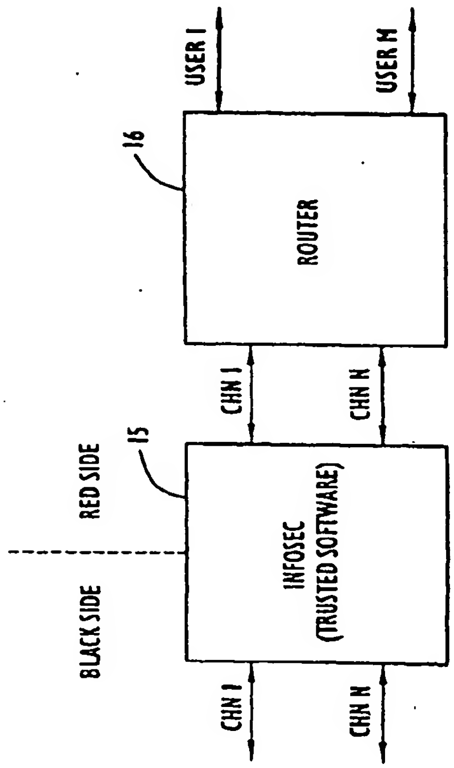

BLACK SIDE
RED SIDE
15
16
INFOSEC
(TRUSTED SOFTWARE)
ROUTER
CHN 1
CHN N
USER 1
USER M

FIG.2

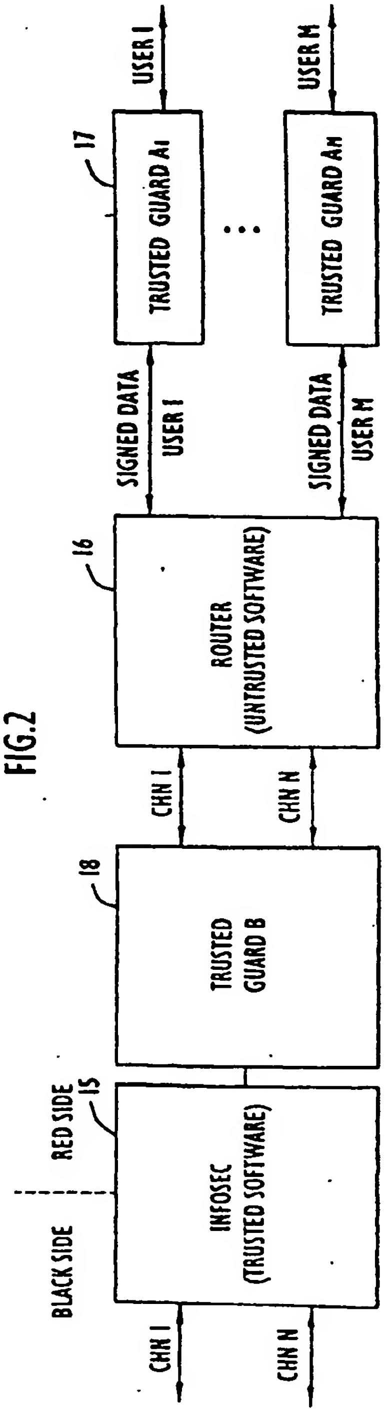

BLACK SIDE
RED SIDE
15
18
16
17
INFOSEC
(TRUSTED SOFTWARE)
TRUSTED
GUARD B
ROUTER
(UNTRUSTED SOFTWARE)
TRUSTED GUARD A1
TRUSTED GUARD AM
CHN 1
CHN N
SIGNED DATA
USER 1
USER M

FIG. 3

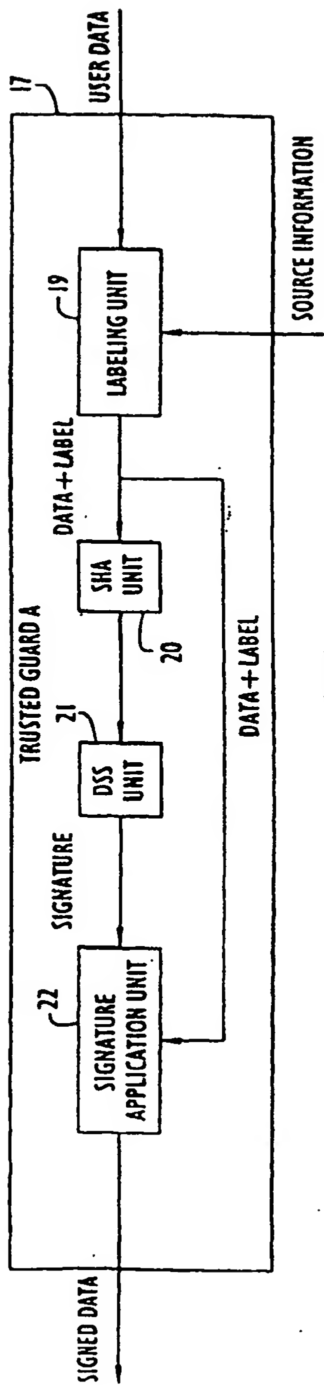

17
USER DATA
TRUSTED GUARD A
LABELING UNIT
19
SOURCE INFORMATION
DATA+LABEL
SHA UNIT
20
21
DSS UNIT
DATA+LABEL
SIGNATURE
22
SIGNATURE APPLICATION UNIT
SIGNED DATA

FIG.4

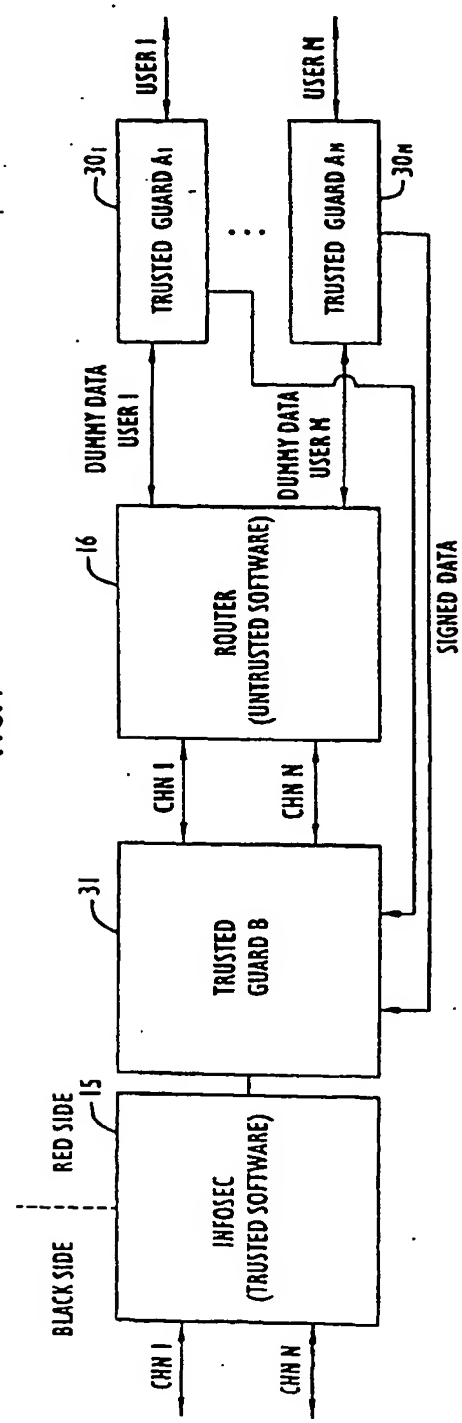

USER I
USER N
30I
TRUSTED GUARD AI
30N
TRUSTED GUARD AN
DUMMY DATA USER I
DUMMY DATA USER N
16
ROUTER (UNTRUSTED SOFTWARE)
SIGNED DATA
CHN I
CHN N
31
TRUSTED GUARD B
RED SIDE
15
BLACK SIDE
INFOSEC (TRUSTED SOFTWARE)
CHN I
CHN N

FIG. 6

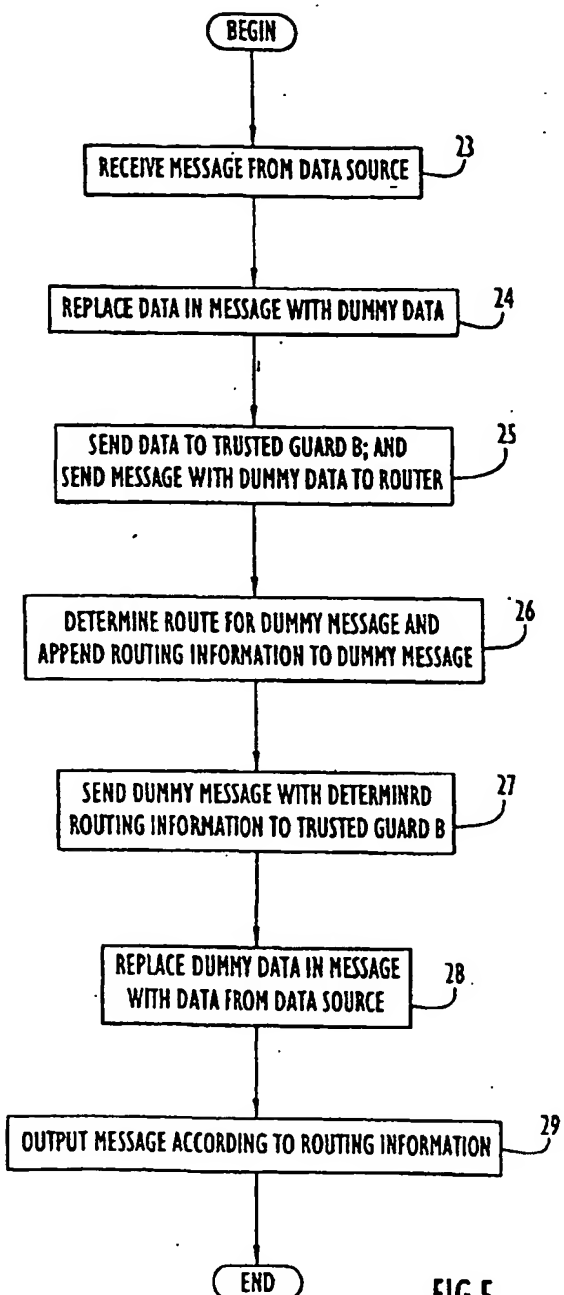

BEGIN
RECEIVE MESSAGE FROM DATA SOURCE
23
REPLACE DATA IN MESSAGE WITH DUMMY DATA
24
SEND DATA TO TRUSTED GUARD B; AND SEND MESSAGE WITH DUMMY DATA TO ROUTER
25
DETERMINE ROUTE FOR DUMMY MESSAGE AND APPEND ROUTING INFORMATION TO DUMMY MESSAGE
26
SEND DUMMY MESSAGE WITH DETERMINRD ROUTING INFORMATION TO TRUSTED GUARD B
27
REPLACE DUMMY DATA IN MESSAGE WITH DATA FROM DATA SOURCE
28
OUTPUT MESSAGE ACCORDING TO ROUTING INFORMATION
29
END

FIG.5

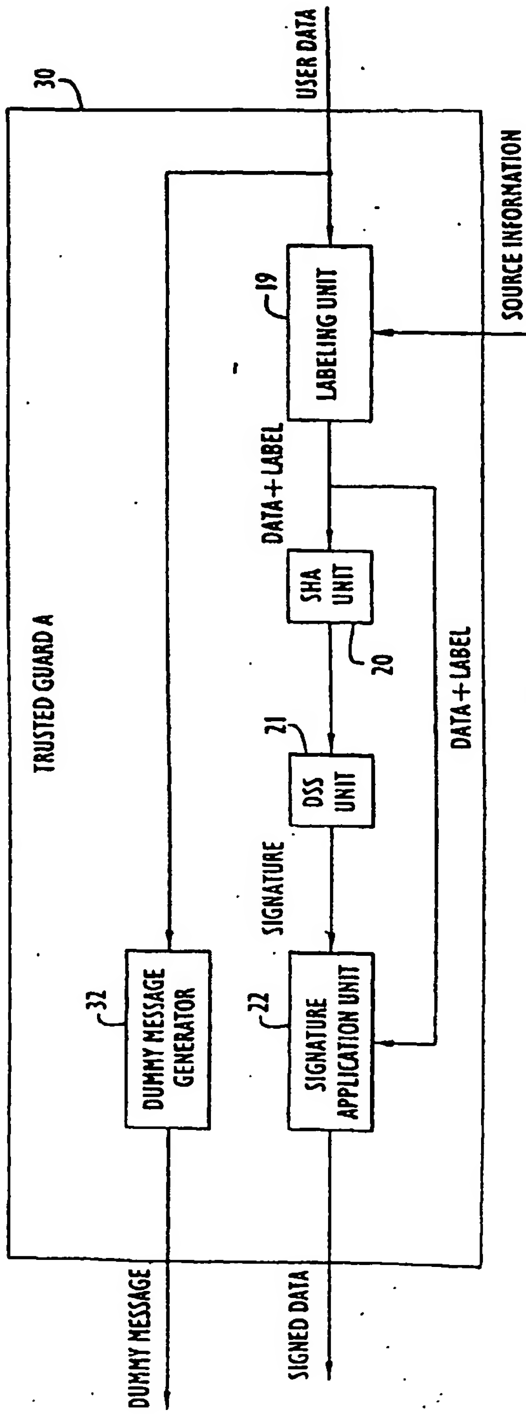

30
USER DATA
TRUSTED GUARD A
SOURCE INFORMATION
19
LABELING UNIT
DATA+LABEL
SHA UNIT
20
DATA+LABEL
21
DSS UNIT
SIGNATURE
32
DUMMY MESSAGE GENERATOR
22
SIGNATURE APPLICATION UNIT
DUMMY MESSAGE
SIGNED DATA

FIG.7

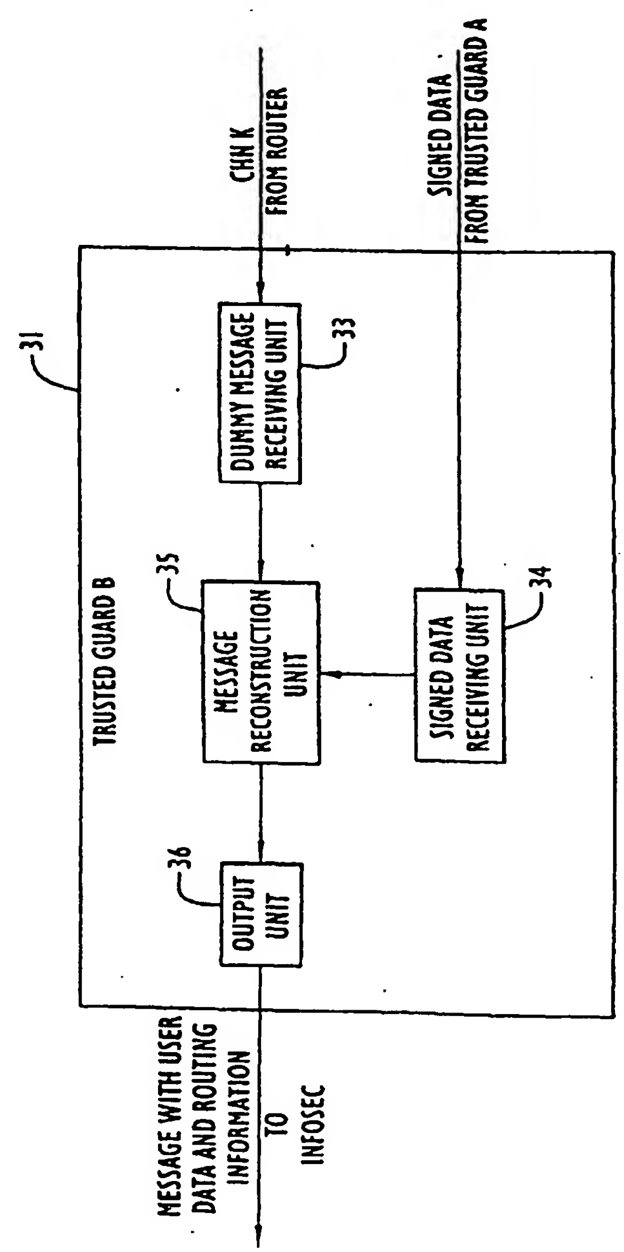

TRUSTED GUARD B
31
CHN K
FROM ROUTER
SIGNED DATA
FROM TRUSTED GUARD A
DUMMY MESSAGE
RECEIVING UNIT
33
MESSAGE
RECONSTRUCTION
UNIT
35
SIGNED DATA
RECEIVING UNIT
34
OUTPUT
UNIT
36
MESSAGE WITH USER
DATA AND ROUTING
INFORMATION
TO
INFOSEC

FIG.8

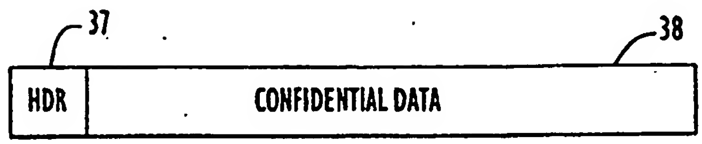



FIG.9A

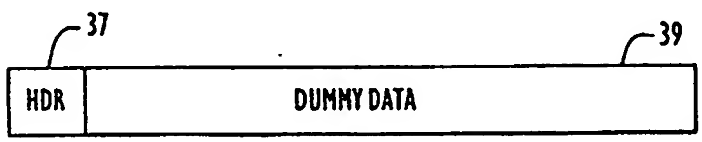



FIG.9B

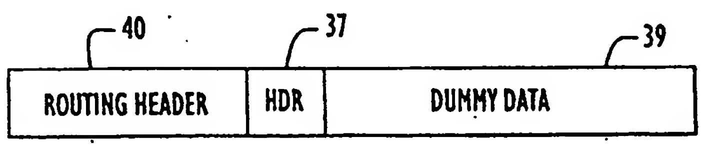



FIG.9C

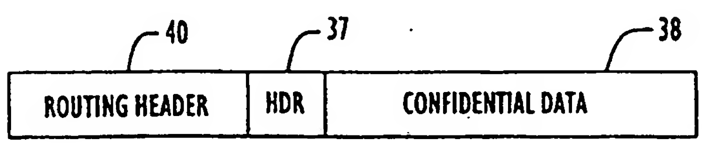



FIG.9D

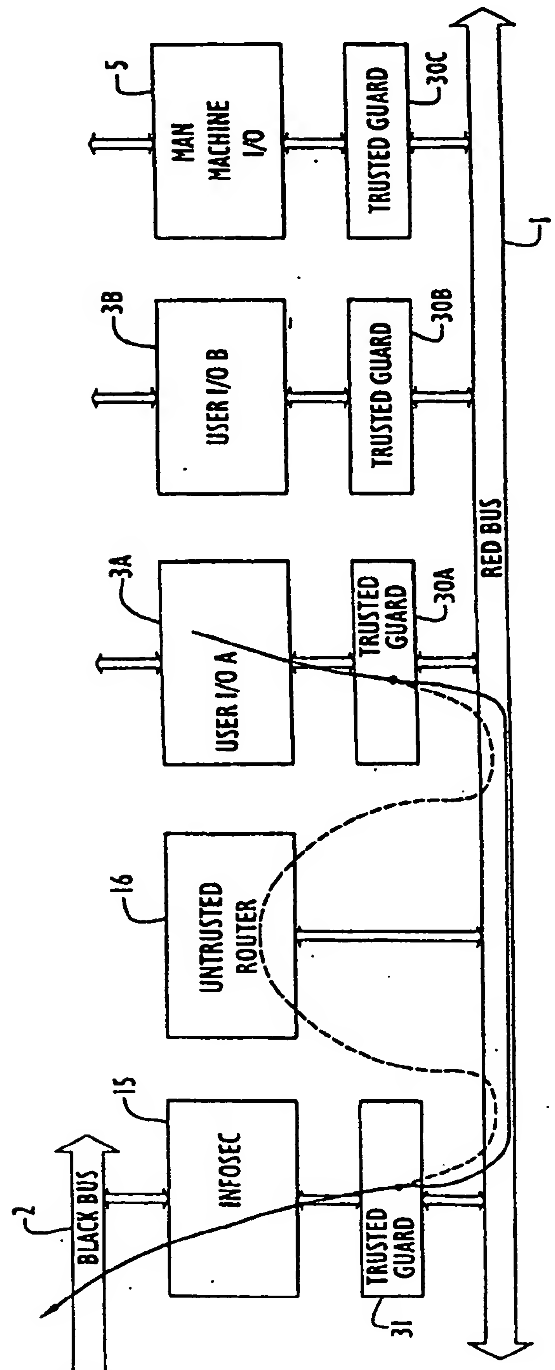

MAN
MACHINE
I/O
5
TRUSTED GUARD
30C
USER I/O B
3B
TRUSTED GUARD
30B
1
RED BUS
USER I/O A
3A
TRUSTED GUARD
30A
UNTRUSTED
ROUTER
16
INFOSEC
15
BLACK BUS
2
TRUSTED GUARD
31

FIG.10A

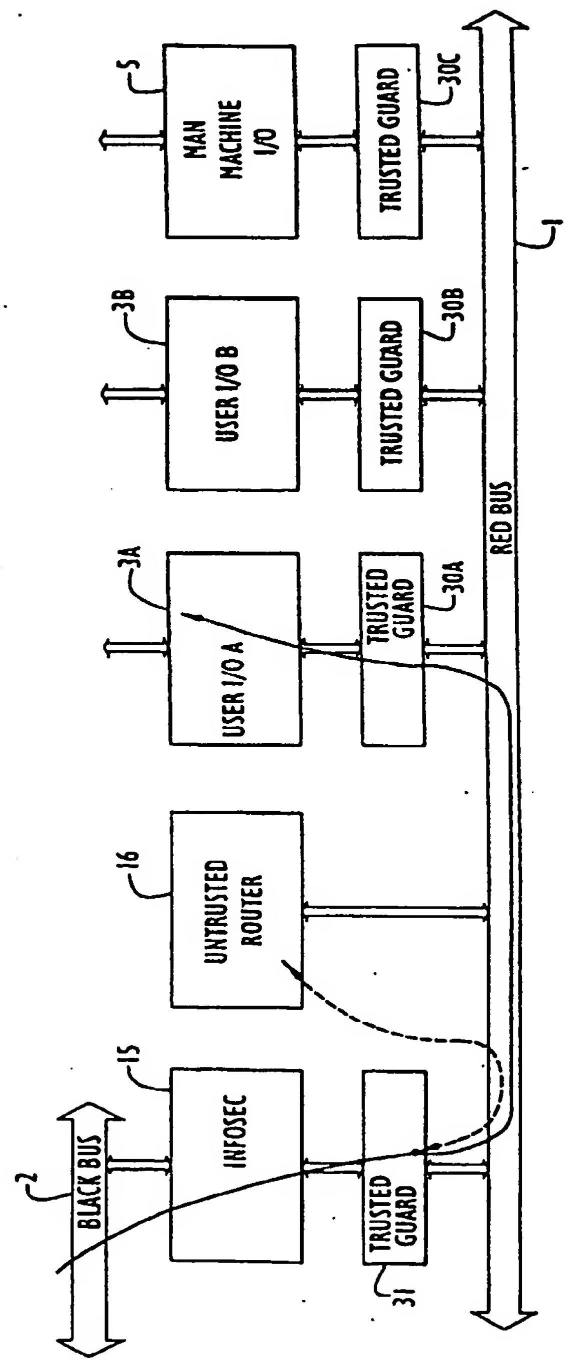

MAN MACHINE I/O
5
TRUSTED GUARD
30C
USER I/O B
3B
TRUSTED GUARD
30B
USER I/O A
3A
TRUSTED GUARD
30A
UNTRUSTED ROUTER
16
INFOSEC
15
TRUSTED GUARD
31
BLACK BUS
2
RED BUS
1

FIG.10B

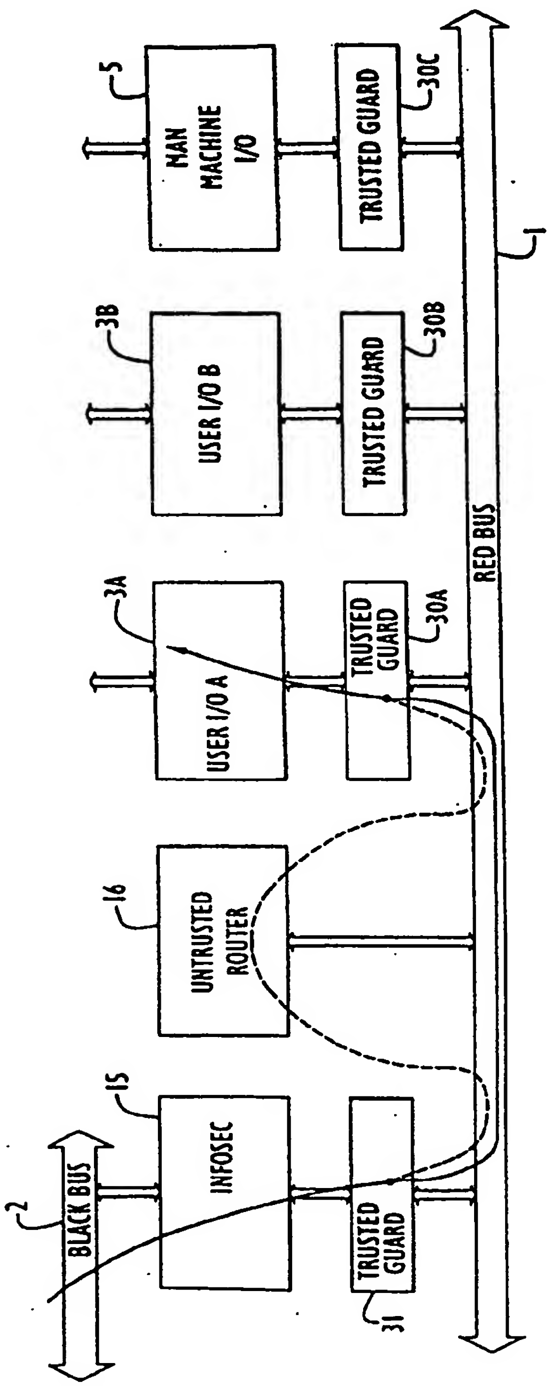
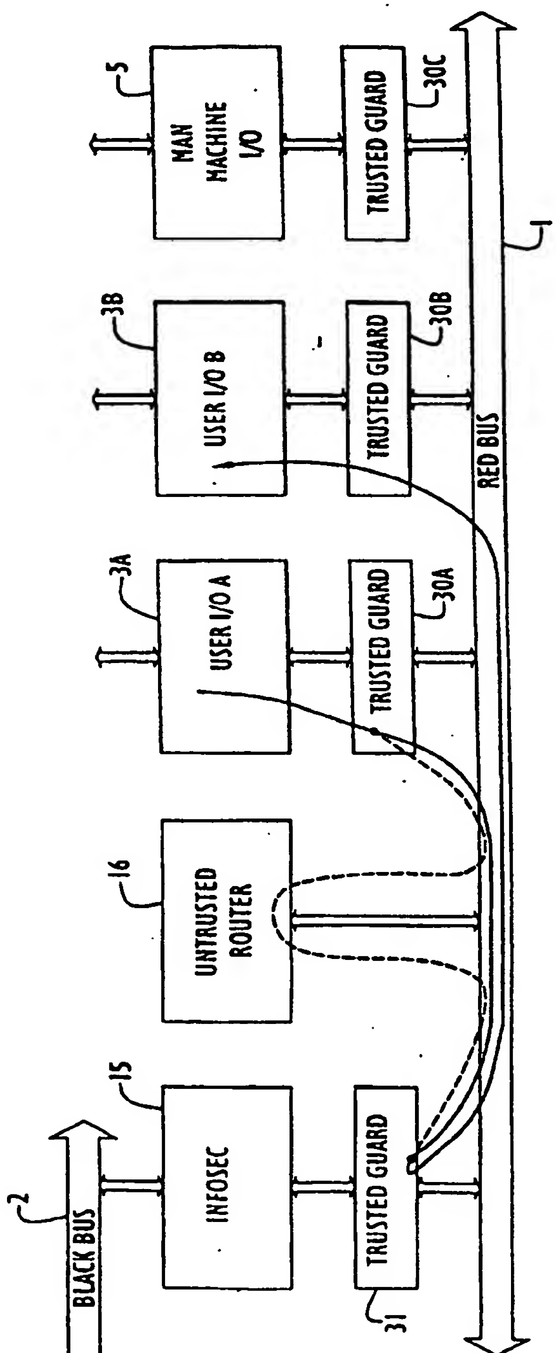

5
MAN MACHINE I/O
TRUSTED GUARD
30C
3B
USER I/O B
TRUSTED GUARD
30B
3A
USER I/O A
TRUSTED GUARD
30A
16
UNTRUSTED ROUTER
15
INFOSEC
TRUSTED GUARD
31
2
BLACK BUS
RED BUS
1

FIG.10C



BLACK BUS
2
INFOSEC
15
TRUSTED GUARD
31
UNTRUSTED ROUTER
16
USER I/O A
3A
TRUSTED GUARD
30A
USER I/O B
3B
TRUSTED GUARD
30B
MAN MACHINE I/O
5
TRUSTED GUARD
30C
RED BUS
1


FIG.10D

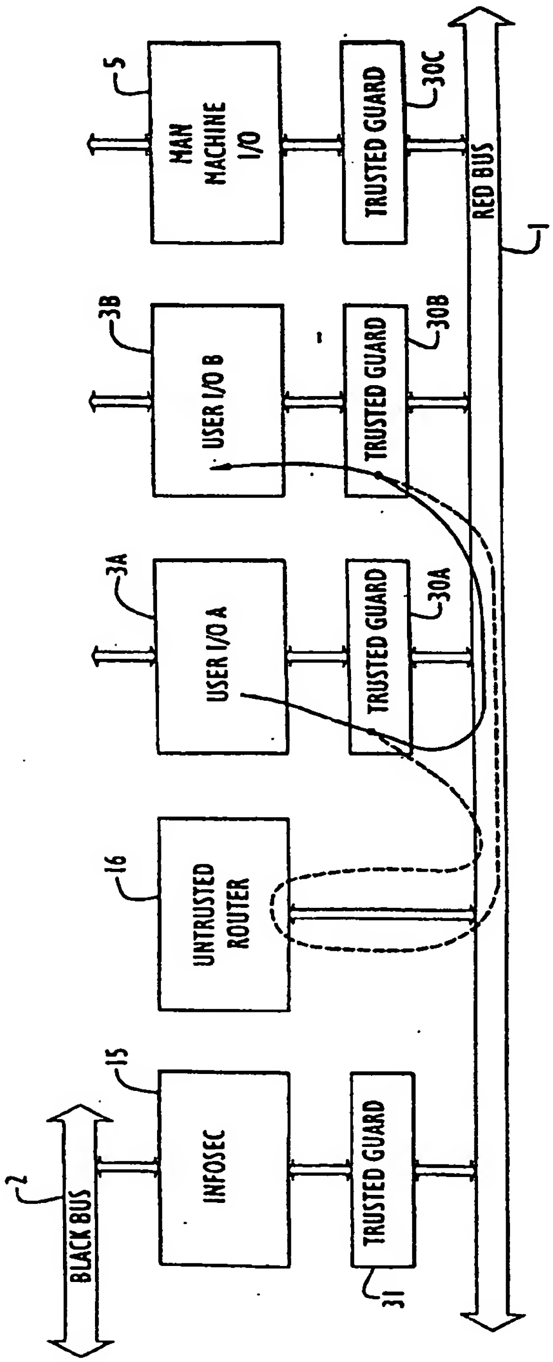

2
BLACK BUS
15
INFOSEC
TRUSTED GUARD
31
16
UNTRUSTED ROUTER
3A
USER I/O A
TRUSTED GUARD
30A
3B
USER I/O B
TRUSTED GUARD
30B
5
MAN MACHINE I/O
TRUSTED GUARD
30C
RED BUS
1

FIG.10E

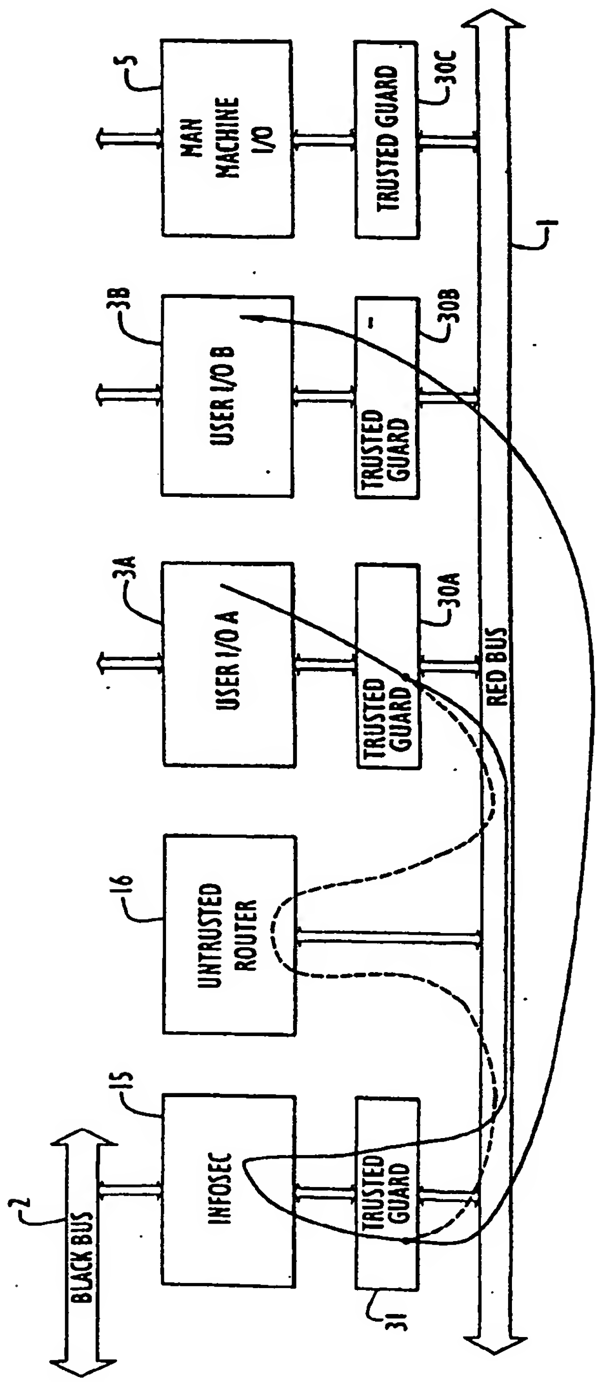

5
MAN MACHINE I/O
TRUSTED GUARD
30C
3B
USER I/O B
TRUSTED GUARD
30B
3A
USER I/O A
TRUSTED GUARD
30A
RED BUS
1
16
UNTRUSTED ROUTER
15
INFOSEC
TRUSTED GUARD
31
2
BLACK BUS

FIG.10F

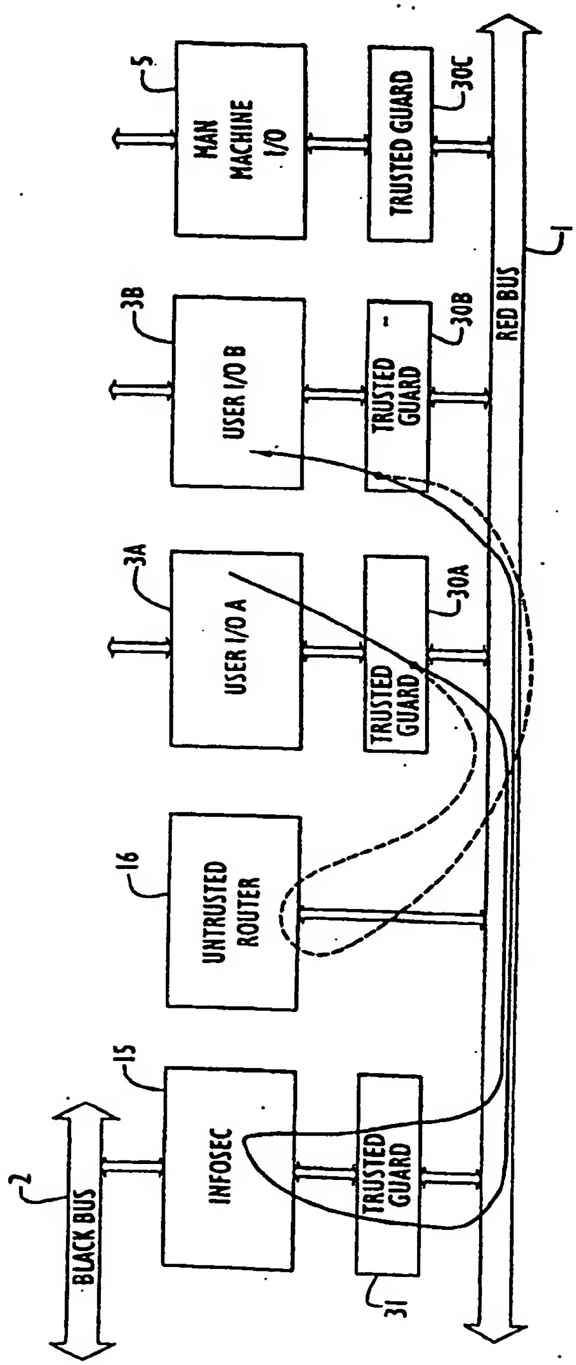

MAN MACHINE I/O
5
TRUSTED GUARD
30C
USER I/O B
3B
TRUSTED GUARD
30B
USER I/O A
3A
TRUSTED GUARD
30A
UNTRUSTED ROUTER
16
INFOSEC
15
TRUSTED GUARD
31
BLACK BUS
2
RED BUS
1

FIG.10G